ABSTRACT OF THE DISCLOSURE

A cryptosystem includes an encrypting device, a communication path, and a decrypting arithmetic device. Key generation means in the encrypting device generate a public key $\{g_1, g_2\}$ as random numbers respectively including the power of (p-1) and the power of (q-1) and decrypt a message m using the Fermat's little theorem and the Chinese remainder theorem. This makes it possible to suggest an extremely simple cryptosystem, which is simplified by reducing the amount of computations for encryption and decryption and enables encryption and decryption by simple calculations, while maintaining a security equivalent to the RSA encryption scheme.